1 Билет №17. Характеристика поля

Определение

Пусть K — поле.

• Положим $\underline{k} := \underbrace{1+1+\cdots+1}_{k}$ для $k \in \mathbb{N}$ и $\underline{k} := -(\underbrace{1+1+\cdots+1}_{-k})$ для отрицательных $k \in \mathbb{Z}$, а также $\underline{0} = 0$.

• Если существует такие $k \in \mathbb{N}$, что $\underline{k} = 0$, то характеристика поля $\mathrm{char}(K)$ равна наименьшему из таких чисел.

• Если же таких натуральных чисел нет, то считается, что $\mathrm{char}(K) = 0$.

То есть $k = \underbrace{1+\ldots+1}_{k} = 0$. Характеристики полей $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ равны нулю. Характеристика поля вычетов $\mathbb{Z}_p$ равна p.

• Несложно проверить, что $\underline{a} + \underline{b} = \underline{a+b}$.

• Раскрыв скобки по дистрибутивности, можно убедиться в том, что $\underline{a} \cdot \underline{b} = \underline{ab}$.

Лемма 15

Пусть K — поле и $\mathrm{char}(K) = p \neq 0$. Тогда $p \in \mathbb{P}$.

Доказательство. • Пусть $p = ab$, где $1 < a < p$ и $1 < b < p$.

• Тогда $\underline{a} \cdot \underline{b} = \underline{ab} = \underline{p} = 0$.

• Так как K — поле, отсюда следует, что хотя бы одно из чисел $\underline{a}$ и $\underline{b}$ равно 0, что противоречит определению характеристики поля. □

$0 = \underbrace{1+\ldots+1}_{p} = \underbrace{(1+\ldots+1)}_{a}\underbrace{(1+\ldots+1)}_{b}$. Так как $a < p$ и $b < p$, то $a \neq 0$ и $b \neq 0$.

2 Билет №18. Теорема о подполе

Теорема 4

Пусть K — поле.

1) *Если $\mathrm{char}(K) = p \in \mathbb{P}$, то отображение $\varphi : \mathbb{Z}/p\mathbb{Z} \to K$, заданное формулой $\varphi(\overline{m}) = \underline{m}$ (для $m \in \mathbb{Z}$) — мономорфизм полей. В частности, K имеет подполе $\mathbb{Z}/p\mathbb{Z}$.*

2) *Если $\mathrm{char}(K) = 0$, то отображение $\varphi : \mathbb{Q} \to K$, заданное формулой $\varphi(\frac{a}{b}) = \frac{\underline{a}}{\underline{b}}$ (для $a, b \in \mathbb{Z}$, $b \neq 0$)— мономорфизм полей. В частности, K имеет подполе $\mathbb{Q}$.*

Доказательство. 1) Отображение $\psi : \mathbb{Z} \to K$, заданное формулой $\psi(m) := \underline{m}$, очевидно, является гомоморфизмом колец.

- $\ker(\psi) = \{m \in \mathbb{Z} \ : \ \underline{m} = 0\}$ — идеал в $\mathbb{Z}$. НУО, $\ker(\psi) = q\mathbb{Z}$.
- Тогда $\underline{m} = 0 \iff m \vdots q$, то есть, $\mathrm{char}(K) = q$. Значит, $q = p$ и $\ker(\psi) = p\mathbb{Z}$.
- По Теореме 2 (о гомоморфизме колец), отображение $\overline{\psi} : \mathbb{Z}/p\mathbb{Z} \to K$, заданное формулой $\overline{\psi}(\overline{m}) = \underline{m}$ — изоморфизм между $\mathbb{Z}/p\mathbb{Z}$ и $\mathrm{Im}(\psi)$ — подполем K.

Вспомним обозначения. Множество всех чисел, сравнимых с a по модулю m, называется классом вычетов a по модулю m, и обычно обозначается $\bar{a}_m$. Таким образом, сравнение $a \equiv_m b$ равносильно равенству классов вычетов $\bar{a}_m = \bar{b}_m$. Множество всех классов вычетов по модулю m обозначается $\mathbb{Z}_m$ или $\mathbb{Z}/m\mathbb{Z}$ или $\mathbb{Z}/(m)$.

Смысл первого утверждения заключается в том, что если характеристикой поля является простое число, то мы имеем инъекцию в отображении из класса вычетов по модулю p в $\underline{m}$, (числа, кратные m, в K равны нулю).

Во втором утверждении нам говорят, что если характеристика поля равна нулю, то у нас подполем является $\mathbb{Q}$. Замечание: любые $\underline{a}$ и $\underline{b}$ не равны нулы.

В доказательствах обоих утверждений приходим к выводу, что образ отображения и есть нужное нам подполе.

2) • В этом случае $\forall m \in \mathbb{N}\ \underline{m} \neq 0$, то есть, $\mathrm{char}(K) = 0$.

- Определим отображение $\varphi : \mathbb{Q} \to K$ формулой $\varphi(\frac{a}{b}) := \frac{\underline{a}}{\underline{b}}$ (при $b \neq 0$).
- Проверим корректность. Пусть $\frac{a}{b} = \frac{c}{d} \iff ad = bc$ (здесь $b, d \neq 0$).
- Тогда по дистрибутивности в поле K имеем $\underline{a} \cdot \underline{d} = \underline{b} \cdot \underline{c} \iff \frac{\underline{a}}{\underline{b}} = \frac{\underline{c}}{\underline{d}}$.
- Проверим, что φ — гомоморфизм:
  - $\varphi(\frac{a}{b}) \cdot \varphi(\frac{c}{d}) = \frac{\underline{a}}{\underline{b}} \cdot \frac{\underline{c}}{\underline{d}} = \frac{\underline{a} \cdot \underline{c}}{\underline{b} \cdot \underline{d}} = \varphi(\frac{ac}{bd}) = \varphi(\frac{a}{b} \cdot \frac{c}{d})$.
  - $\varphi(\frac{a}{b}) + \varphi(\frac{c}{d}) = \frac{\underline{a}}{\underline{b}} + \frac{\underline{c}}{\underline{d}} = \frac{\underline{a} \cdot \underline{d} + \underline{b} \cdot \underline{c}}{\underline{b} \cdot \underline{d}} = \varphi(\frac{ad+bc}{bd}) = \varphi(\frac{a}{b} + \frac{c}{d})$.
- Так как $\mathbb{Q}$ — поле и φ принимает не только нулевые значения, $\ker(\varphi) = \{0\}$.
- Значит, $\mathrm{Im}(\varphi)$ — подполе K, изоморфное $\mathbb{Q}$. □

Следствие 3

Все поля из $p \in \mathbb{P}$ элементов изоморфны $\mathbb{Z}/p\mathbb{Z}$.